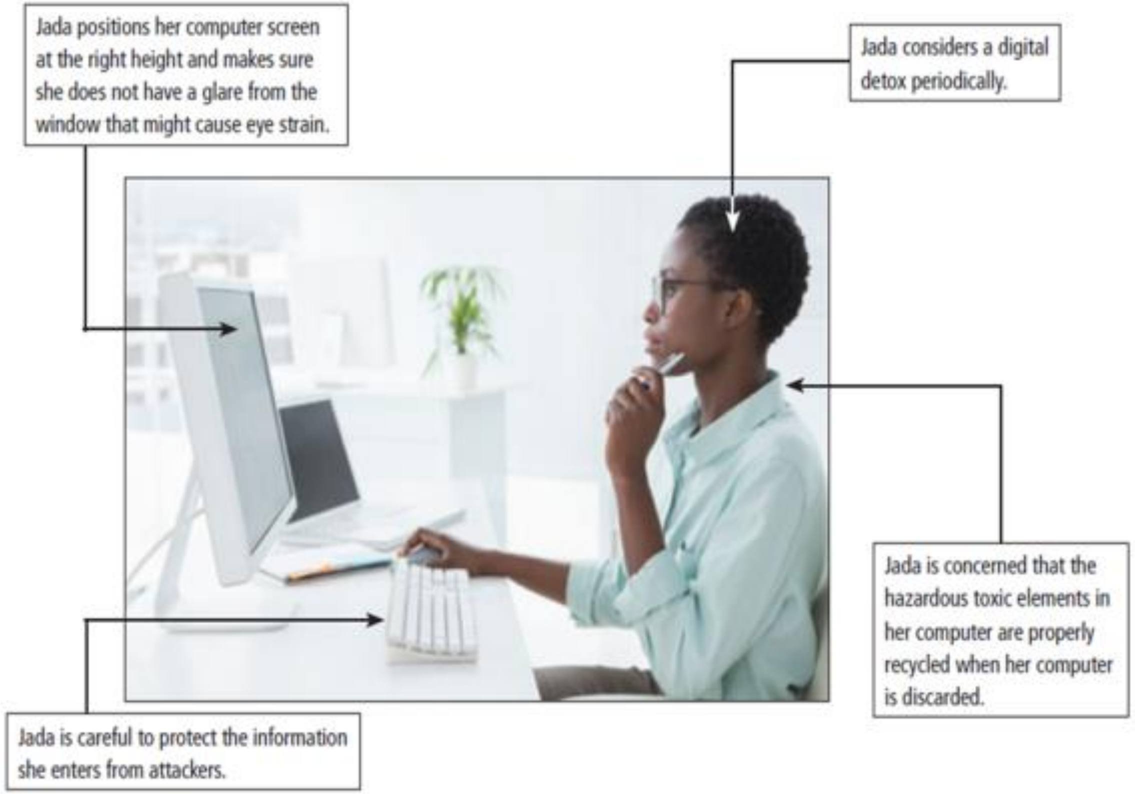
Ch5

Digital Security, Ethics, and Privacy: Avoiding and Recognizing Threats

Dr. Jian-Ren Hou

Risks Associated with Technology Use

- A **digital security risk** is any event or action that could cause a loss of or damage to computer or mobile device hardware, software, data, information, or processing capability.
- **Types of digital security risks** include threats to our information, physical health, mental health, and the environment.



Jada positions her computer screen at the right height and makes sure she does not have a glare from the window that might cause eye strain.

Jada considers a digital detox periodically.

Jada is concerned that the hazardous toxic elements in her computer are properly recycled when her computer is discarded.

Jada is careful to protect the information she enters from attackers.

Figure 5-1 You can protect yourself from digital security risks.

Cybercrimes and Criminals

- State-sponsored attackers are employed by the government to launch computer attacks against their enemies through **nation-state actors.**
- The term, **cyberwarfare,** describes an attack whose goal ranges from disabling a government’s computer network to crippling a country.
- These attackers try to steal and then use your credit card numbers, online financial account information, or Social Security numbers using data mining.
- **Social engineering** is a category of attack that attempts to trick the victim into giving valuable information to the attacker.
  - Examples include hoaxes and phishing

Risks Associated with Technology Use

- Any illegal act involving the use of a computer or related devices is generally referred to as a **computer crime** and the term **cybercrime** refers to online or Internet-based illegal acts, such as distributing malicious software or committing identity theft.
- Software used by cybercriminals is called **crimeware. Cybersecurity** is the practice of protection against digital threats, including unauthorized or illegal access to data.
- **Digital forensics, or cyber forensics** is the discovery, collection, and analysis of evidence found on computers and networks.
- A **digital forensics examiner** must have knowledge of the law, technical experience with many types of hardware and software products, superior communication skills, familiarity with corporate structures and policies, a willingness to learn and update skills, and a knack for problem-solving.

Risks Associated with Technology Use

- A **digital detox** is a period of time during which an individual refrains from using technology.
- The **dark web** is a part of the web that is accessed using specialized software, where users and website operators can remain anonymous while performing illegal actions.
- **Script kiddies** are individuals who want to attack computers.
- A **hacker** is a person who intends to access a computer system without permission.
- A **cracker** is someone who accesses a computer or network illegally but has the intent of destroying data, stealing information, or other malicious action.
- **Hacktivists** are attackers who are strongly motivated by principles or beliefs.
- **Cyberterrorists** attack a nation’s computer networks, like the electrical power grid, to cause disruption and panic among citizens.

Cybercrimes and Criminals

Table 5-1 Social engineering principles.

Principle	Description	Example
Authority	Directed by someone impersonating authority figure or falsely citing their authority	“I’m the CEO calling.”
Intimidation	To frighten and coerce by threat	“If you don’t reset my password, I will call your supervisor.”
Consensus	Influenced by what others do	“I called last week and your colleague reset my password.”
Scarcity	Something is in short supply	“I can’t waste time here.”
Urgency	Immediate action is needed	“My meeting with the board starts in five minutes.”
Familiarity	Victim well-known and well-received	“I remember reading a good evaluation on you.”
Trust	Help a person known to you	“You know who I am.”

Ethics and Society

- The standards that determine whether an action is good or bad are known as ethics.
- **Technology ethics** are the moral guidelines that govern the use of computers, mobile devices, information systems, and related technologies.
- Frequently discussed areas of computer ethics include information accuracy, intellectual property rights, and green computing.

Ethics and Society

Information Accuracy

- Information accuracy is a concern today because many users access information maintained by other people or companies, such as on the Internet.
- With graphics equipment and software, users can easily digitize photos and then add, change, or remove images.

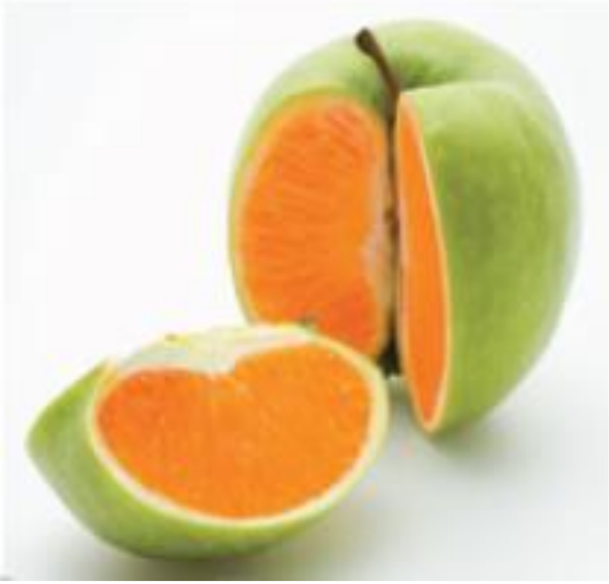
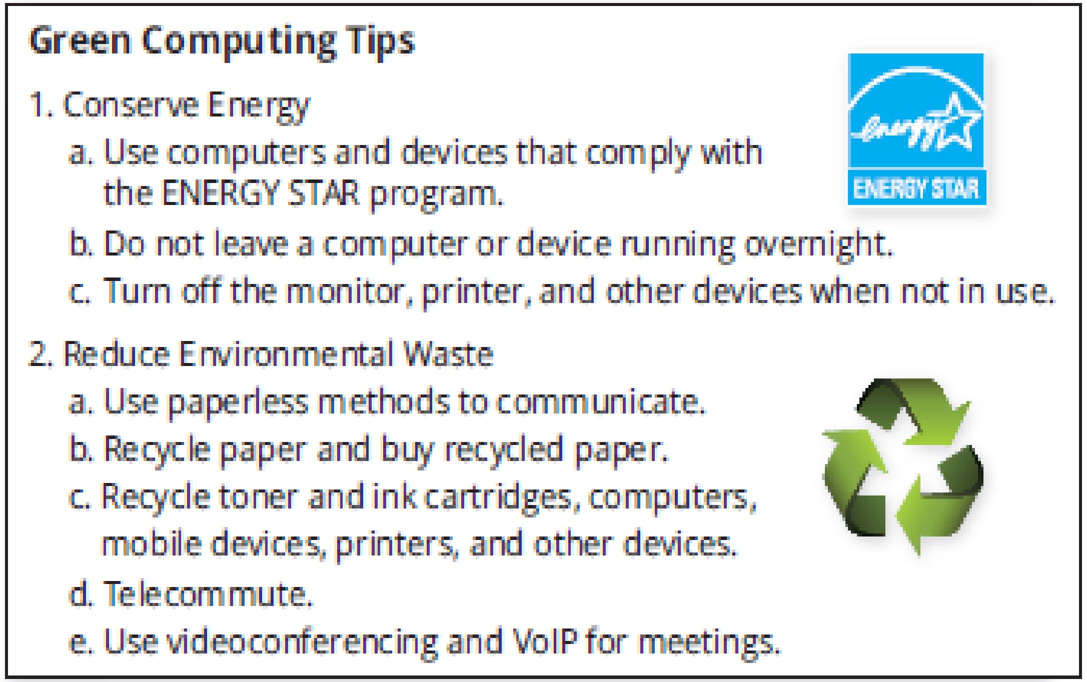


Figure 5-3 A digitally edited photo that shows a fruit that looks like an apple on the outside and an orange on the inside.

Ethics and Society

Green Computing

- **Green computing** involves reducing electricity and environmental waste while using computers, mobile devices, and related technologies.
- Organizations can implement a variety of measures to reduce electrical waste.



Green Computing Tips

1. Conserve Energy
   a. Use computers and devices that comply with the ENERGY STAR program.
   b. Do not leave a computer or device running overnight.
   c. Turn off the monitor, printer, and other devices when not in use.
2. Reduce Environmental Waste
   a. Use paperless methods to communicate.
   b. Recycle paper and buy recycled paper.
   c. Recycle toner and ink cartridges, computers, mobile devices, printers, and other devices.
   d. Telecommute.
   e. Use videoconferencing and VoIP for meetings.

Figure 5-5 A list of suggestions to make computing healthy for the environment.

Internet and Network Attacks

- Information transmitted over networks has higher degree of a security risk than information kept on an organization’s premises.
  - These types of attacks can affect your privacy, personal information, finances, and more.
- **Malware** is short for malicious software which consists of programs that act without a user’s knowledge and deliberately alter the operations of computers and mobile devices.
- A common way that computers and mobile devices become infected with viruses and other malware is through users opening infected email attachments.

Internet and Network Attacks

Table 5-2 Common types of malware.

Type	Description
Adware	A program that displays an online advertisement in a banner, pop-up window, or pop-under window on web pages, email messages, or other Internet services
Ransomware	A program that blocks or limits access to a computer, phone, or file until the user pays a specified amount of money
Rootkit	A program that hides in a computer or mobile device and allows someone from a remote location to take full control of the computer or device
Spyware	A program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online
Trojan horse	A program that hides within or looks like a legitimate program. Unlike a virus or worm, a Trojan horse does not replicate itself to other computers or devices
Virus	A potentially damaging program that affects, or infects, a computer or mobile device negatively by altering the way the computer or device works without the user's knowledge or permission
Worm	A program that copies itself repeatedly, for example, in memory or on a network, using up resources and possibly shutting down the computer, device, or network

Internet and Network Attacks

Botnets

- A compromised computer or device, known as a **zombie,** is one whose owner is unaware that the computer or device is being controlled remotely by an outsider.
- A **botnet,** or zombie army, is a group of compromised computers or mobile devices connected to a network that are used to attack other networks, usually for nefarious purposes.
- A **bot** is a program that performs a repetitive task on a network.
- Cybercriminals install malicious bots on unprotected computers and devices to create botnets.

Internet and Network Attacks

Denial of Service Attacks

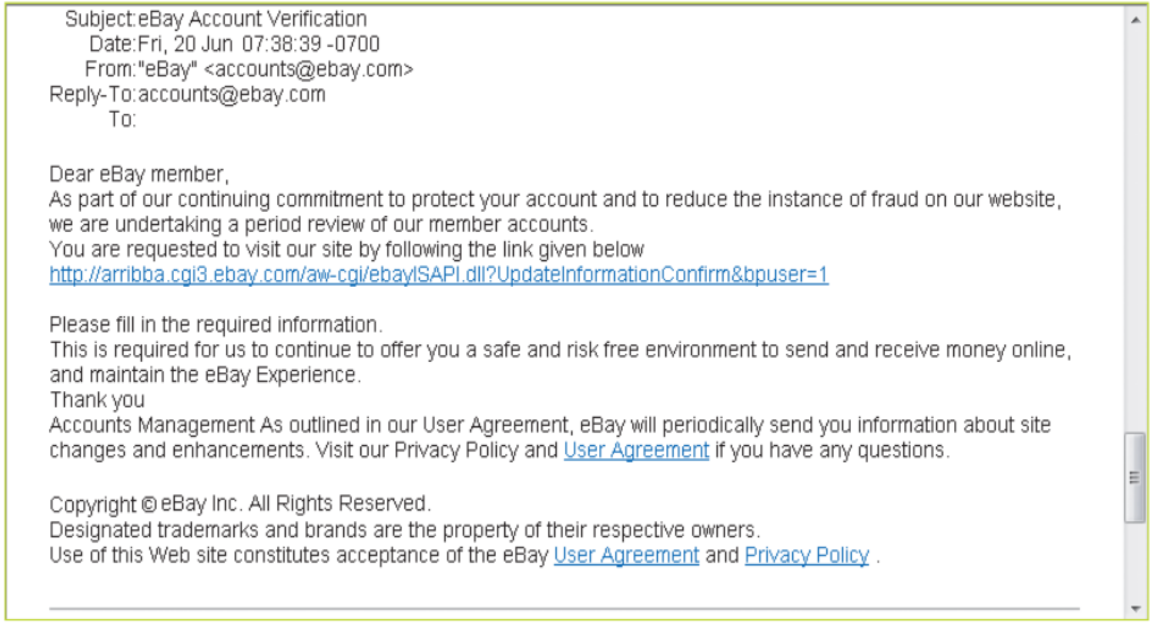
- A **DoS** attack is a type of attack, usually on a server, that is meant to overload the server with network traffic so that it cannot provide necessary services, such as the web or email.
- A more devastating type of DoS attack is the distributed DoS (**DDoS**) attack in which multiple computers, such as a zombie army, are used to attack a server or other network resource.
- The damage caused by a DoS or DDoS attack usually is extensive.

Back Doors

- A back door is a program or set of instructions in a program that allows users to bypass security controls when accessing a program, computer, or network.
- A rootkit can be a back door.
- Some worms leave back doors, which have been used to spread other worms or to distribute spam from the unsuspecting victim’s computers.
- Programmers often build back doors into programs during system development to save development time.

Internet and Network Attacks

- **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate to a victim's computer or network.
- Two common types of spoofing schemes are **IP** and **address spoofing**.
  - ✓ **IP spoofing** occurs when an intruder computer tricks a network into believing its IP address is associated with a trusted source.
  - ✓ **Address spoofing** occurs when the sender's email address or other components of an email header are altered.



Subject:eBay Account Verification
Date:Fri, 20 Jun 07:38:39 -0700
From:"eBay" <accounts@ebay.com>
Reply-To:accounts@ebay.com
To:

Dear eBay member,
As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.
You are requested to visit our site by following the link given below
http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1

Please fill in the required information.
This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.
Thank you
Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy .

Figure 5-5 Spoofers alter the components and header of an email message so that it appears the message originated from a different sender.

Internet and Network Attacks

Practices for Protection from Viruses and Other Malware

- Use virus protection software
- Use a firewall
- Be suspicious of all unsolicited email and text messages
- **Disconnect** your computer from the Internet
- Download software with caution
- Before using any removable media, scan it for malware
- Keep current and back up regularly

Secure IT: Protect Yourself and Your Data

- Your **digital footprint** is the record of everything you do online.
- A digital footprint can be nearly impossible to completely erase.
- **Firewalls** and access controls protect data and information on computers and other devices For most computer users, the greatest risk comes from attackers who want to steal their information for their own financial gain.
- The risks you face online when using the Internet or email include:
  - ✓ **Online Banking**
  - ✓ **E-commerce Shopping**
  - ✓ **Fake Websites**
  - ✓ **Social Media Sites**

Secure IT: Protect Yourself and Your Data

- Mobile users today often access their company networks through a **virtual private network (VPN)**.
  - A **VPN** is a private, secure path across a public network that allows authorized users to secure access to a company or other network.
  - A **VPN** provides the mobile user with a secure connection to the company's network server as if the user has a private line.
  - **VPNs** help ensure that data is safe from being intercepted by unauthorized people by encrypting data as it transmits from a laptop, smartphone, or other mobile devices.

Secure IT: Protect Yourself and Your Data

- **Firewalls** protect network resources from outsiders and to restrict employees' access to sensitive data, such as payroll or personnel records.
- A **proxy server** is a server outside the organization's network that controls which communications pass in and out of the organization's network.
- Both Windows and Mac operating systems include firewall capabilities, including monitoring Internet traffic to and from installed applications.

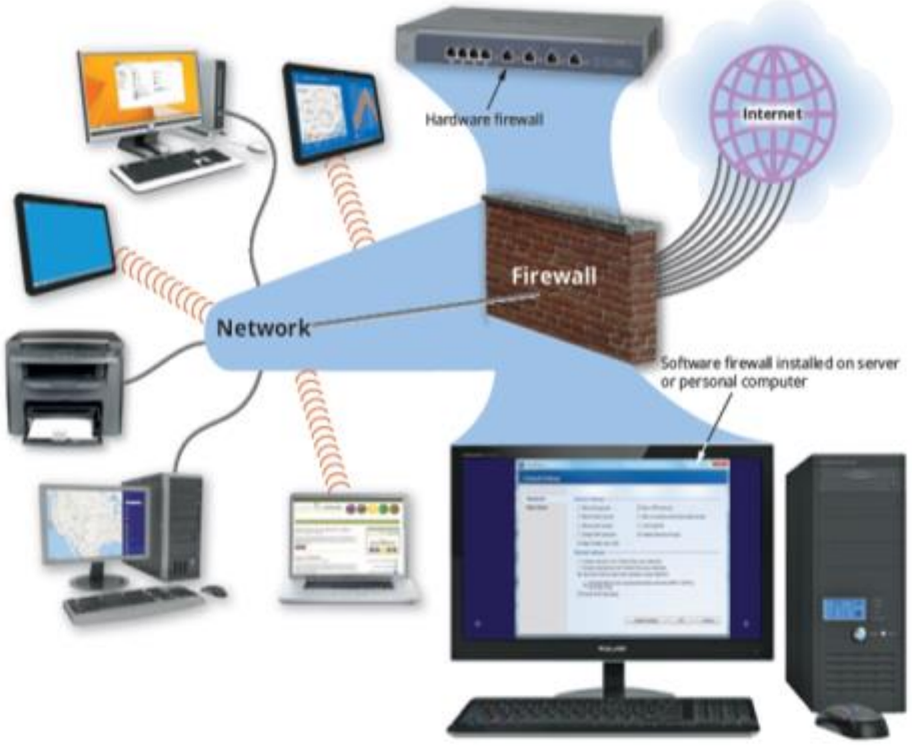


Figure 5-8 How a firewall works.

Wireless Security

Protect Mobile Devices

- Along with the protection of devices from theft, it is also necessary to protect the privacy of your information.
- Some risks from attacks on Wi-Fi networks include the following:
  - ✓ Reading wireless transmissions or viewing or stealing computer data
  - ✓ Injecting malware or downloading harmful content

Precautions

- When using public Wi-Fi, be sure you are connecting to the approved wireless network.
- Limit the type of activity you do on public networks to simple web surfing or watching online videos.
- Accessing online banking sites or sending confidential information that could be intercepted is not a good idea.
- Configuring your Wi-Fi wireless router to provide the highest level of security is an important step.

Wireless Security

Table 5-5 Configuration settings for wireless routers.

Wireless Router Settings	Explanation	Recommended Configuration
Access password	This requires a password to access the configuration settings of the device.	Create a strong password so that attackers cannot access the wireless router and turn off the security settings
Remote management	Remote management allows the configuration settings to be changed from anywhere through an Internet connection.	Turn off remote management so that someone outside cannot access the configuration settings
Service Set Identifier (SSID)	The SSID is the name of the local wireless network.	Change this from the default setting to a value that does not reveal the identity of the owner or the location of the network (such as MyWireNet599342)

Wireless Security

Table 5-5 Configuration settings for wireless routers (continued).

Wireless Router Settings	Explanation	Recommended Configuration
Wi-Fi Protected Access 2 (WPA2) Personal	WPA2 encrypts the wireless data transmissions and also limits who can access the Wi-Fi network.	Turn on WPA2 and set a strong pre-shared key, which must also be entered once on each mobile device
Wi-Fi Protected Setup (WPS)	WPS simplifies setting up the security on a wireless router.	Turn off WPS due to its security vulnerabilities
Guest access	Guest access allows temporary users to access the wireless network without any additional configuration settings.	Turn on guest access when needed and turn it back off when the approved guests leave
Disable SSID broadcasts	This prevents the wireless router from advertising the wireless network to anyone in the area.	Leave SSID broadcasts on; turning them off only provide a very weak degree of security and may suggest to an attacker that your network has valuable information

Wireless Security

Secure Your Wireless Network

The following list provides suggestions for securing your wireless network.

- Immediately upon connecting your wireless access point and/or router, change the password required to access administrative features
- Change the SSID, or network name, from the default to something
- Do not broadcast the SSID
- Enable an encryption method, and specify a strong password
- Enable and configure the Media Access Control (MAC) address control feature; a **MAC address** is a unique hardware identifier for your computer or device
- Choose a secure location for your wireless router so that unauthorized people cannot access it

Information Privacy

- **Authentication** is the process of ensuring that the person requesting access to a computer or other resources is authentic and not an imposter.
- Different methods of authentication are:
  - ✓ Passwords
  - ✓ Biometrics
  - ✓ 2 FA (**Two-Factor Authentication**)
  - ✓ CAPTCHA
  - ✓ Encryption

Information Privacy

Table 5-6 Ten most common passwords.

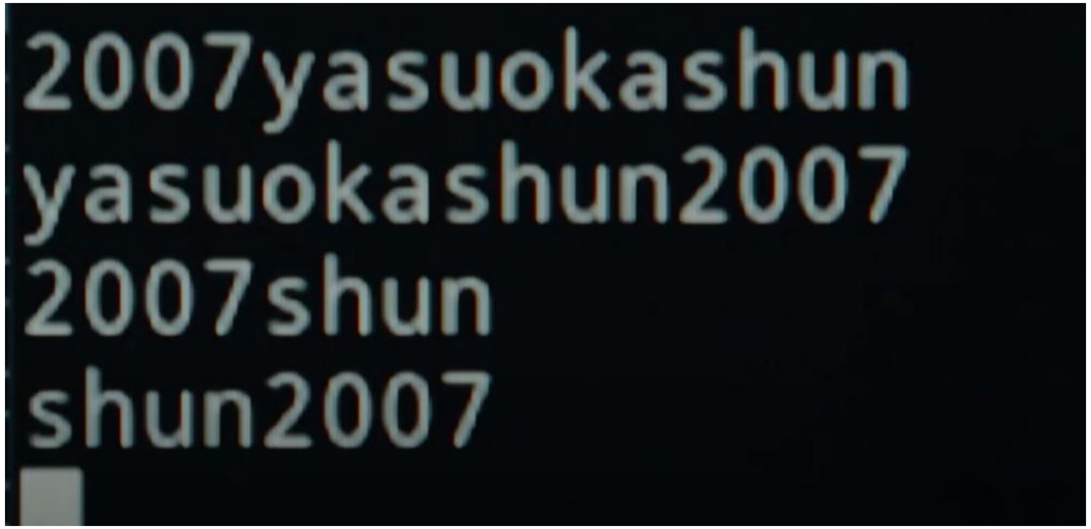
Rank	Password
1	123456
2	123456789
3	qwerty
4	password
5	1111111
6	12345678
7	abc123
8	password1
9	1234567
10	12345

Table 5-7 Numbers of possible passwords.

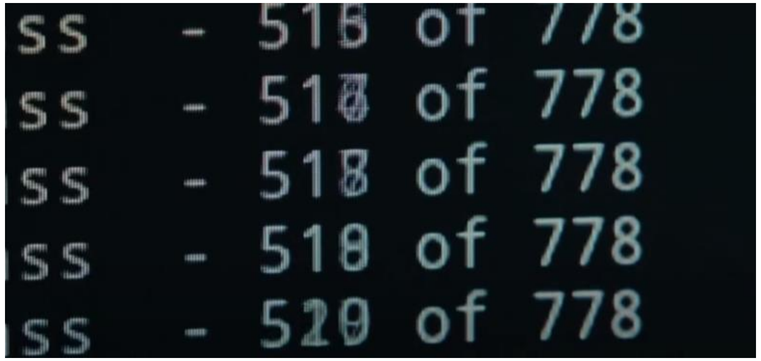
Password length	Number of possible Passwords	Average attempts to Break Password
2	9025	4513
3	857,375	428,688
4	81,450,625	40,725,313
5	7,737,809,375	3,868,904,688
6	735,091,890,625	367,545,945,313

Information Privacy

- Use a **password manager,** which is a program that helps you create and store multiple strong passwords in a single user vault file that is protected by one strong master password.
- **Password managers** use two-step verification and advanced encryption techniques to ensure information is stored securely.



```
2007yasuokashun
yasuokashun2007
2007shun
shun2007
```



```
ss    - 516 of 778
ss    - 517 of 778
ss    - 518 of 778
ss    - 519 of 778
ss    - 520 of 778
```

Information Privacy

- **Two-Factor Authentication** is multiple types of authentication.
- The most common authentication elements that are combined are passwords and codes sent to a cell phone using a text message.
- Its short form is **2FA.**
- It makes authentication stronger.

Figure 5-12 Two-factor authentication.

Information Privacy

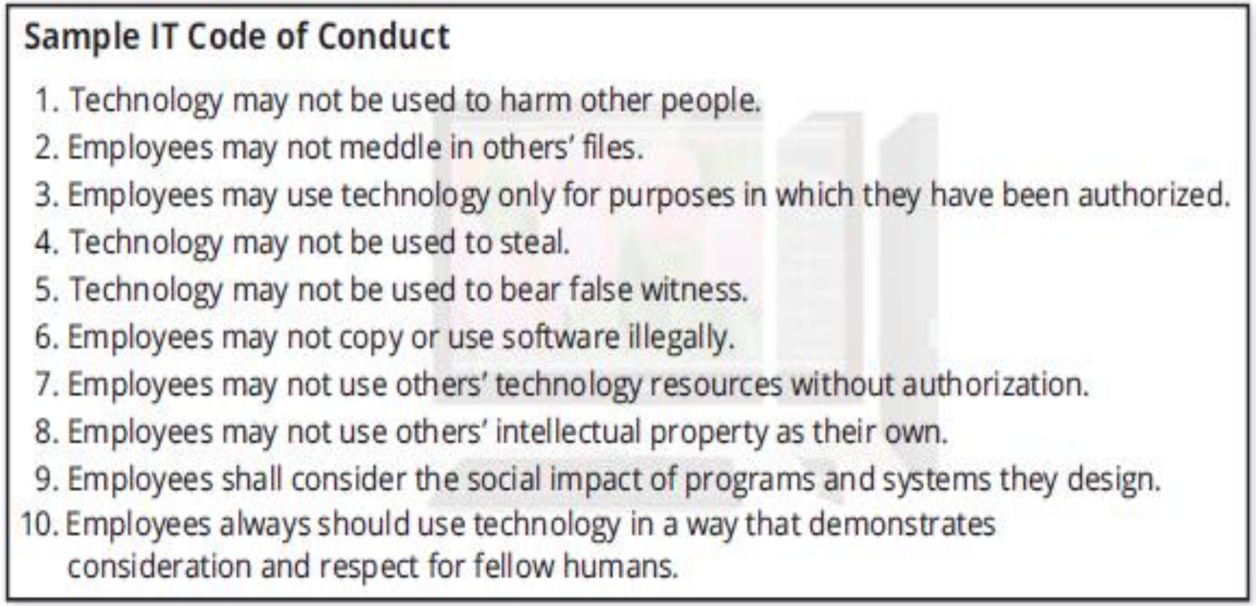
CAPTCHAs

- **CAPTCHA** stands for “Completely Automated Public Turing test to tell Computers and Humans Apart.”
- A **CAPTCHA** is a program developed at Carnegie Mellon University that displays an image containing a series of distorted characters to identify and enter to verify that user input is from humans.

Figure 5-13 CAPTCHAs verify human usage.

How To: Establish Policies to Ensure Safety

- Companies establish **guidelines for use**, occasionally limit access, and possibly oversee employees' activities for unacceptable actions.
- A **code of conduct** is a written guideline that helps determine whether a specification is ethical, unethical or allowed or not allowed.
- An IT code of conduct focuses on the acceptable use of technology.



Sample IT Code of Conduct

1. Technology may not be used to harm other people.
2. Employees may not meddle in others' files.
3. Employees may use technology only for purposes in which they have been authorized.
4. Technology may not be used to steal.
5. Technology may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' technology resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use technology in a way that demonstrates consideration and respect for fellow humans.

Figure 5-14 Sample IT code of conduct.

How To: Establish Policies to Ensure Safety

- **Content filtering** is the process of restricting access to certain materials. Many businesses use content filtering to limit employees’ web access.
- **Web filtering software** are programs that restrict access to specified websites. Some also filter websites that use specific words.

How To: Establish Policies to Ensure Safety

Employee Monitoring

- **Employee monitoring** involves the use of computers, mobile devices, or cameras to observe, record, and review an employee's use of technology, including communications such as email messages, keyboard activity (used to measure productivity), and websites visited.
- Many programs exist that easily allow employers to monitor employees.
- If a company does not have a formal email policy, it can read email messages without employee notification.

How To: Establish Policies to Ensure Safety

Disaster Recovery

- A **disaster recovery plan** is a written plan that describes the steps an organization would take to restore its computer operations in the event of a disaster.
- Each company and each department within an organization usually has its own.
- It typically contains four components: **Emergency plan, Back up plan, Recovery plan, and Test plan**

Emergency Plan

An emergency plan specifies the steps and is organized by type of disaster and includes:

- Names and phone numbers of people and organizations to notify
- Computer equipment procedures and employee evacuation procedures
- Return procedures (who can enter the facility and what actions they are to perform)

How To: Establish Policies to Ensure Safety

Backup Plan

The **backup plan** specifies how to use backup files and equipment to resume computer operations, and includes:

- The location of backup data, supplies, and equipment
- Who is responsible for gathering backup resources and transporting them to an alternate computer facility
- The methods by which data will be restored from cloud storage
- A schedule indicating the order and approximate time each application should be up and running

How To: Establish Policies to Ensure Safety

Recovery Plan:

The recovery plan specifies the actions to restore full computer operations such as replacing hardware or software.

Test Plan:

The test plan includes simulating various levels of disasters and recording the ability to recover.

Ethics and Issues: Inclusivity and Digital Access

Digital Inclusion

- **Digital inclusion** is the movement to ensure that all users, regardless of economic or geographic constraints, have access to the devices, data, and infrastructure required to receive high-speed, accurate, reliable information.
- The goal of **digital inclusion** is to ensure that everyone has access to all the online resources, including education, participation in the local and national government, employment listings and interviews, and health care access.

Ethics and Issues: Inclusivity and Digital Access

Some barriers to digital inclusion include:

- Geographic areas that lack the infrastructure necessary to provide reliable Internet access
- Government restrictions or censorship
- Affordable devices or connections
- Lack of education
- Lack of understanding of the value of technology

Thank You